CompTIA® Security+® (Exam SY0-301)

Course Specifications

Course number: 085707
Course length: 5.0 day(s)
Certification: The CompTIA® Security+® (Exam SY0-301) course is designed to help you prepare for the SY0-301 exam. Attending this course and using this student guide will help you prepare for certification. You should also refer to the exam objectives to see how they map to the course content.

Course Description

Course Objective: You will implement and monitor security on networks, applications, and operating systems, and respond to security breaches.

Target Student: This course is targeted toward the information technology (IT) professional who has networking and administrative skills in Windows®-based Transmission Control Protocol/Internet Protocol (TCP/IP) networks and familiarity with other operating systems, such as Mac OS® X, Unix, or Linux, and who wants to further a career in IT by acquiring a foundational knowledge of security topics; prepare for the CompTIA Security+ Certification examination; or use Security+ as the foundation for advanced security certifications or career roles.

Prerequisites: Basic Windows skills and a fundamental understanding of computer and networking concepts are required. Students can obtain this level of skill and knowledge by taking the following Element K courses: Introduction to Networks and the Internet and any one or more of the following:

- Introduction to Personal Computers: Using Windows 7
- Microsoft® Windows® 7: Level 1

CompTIA A+ and Network+ certifications, or equivalent knowledge, and six to nine months experience in networking, including experience configuring and managing TCP/IP, are strongly recommended. Students can obtain this level of skill and knowledge by taking any of the following Element K courses:

- CompTIA® A+® Certification: A Comprehensive Approach for all 2009 Exam Objectives (Windows® 7)
- CompTIA® Network+® Certification (2009 Objectives)

Additional introductory courses or work experience in application development and programming or in network and operating system administration for any software platform or system are helpful but not required.

Hardware Requirements

To run this course, make sure all equipment is designed for Microsoft® Windows Server® 2008 R2. You will need one computer for each student and one for the instructor. Each computer will need to meet the recommended hardware specifications for Windows Server 2008 R2 as well as the classroom hardware specifications:

- 1.4 gigahertz (GHz) (single 64–bit processor) or 1.3 GHz (dual core).
- 1 gigabyte (GB) of Random Access Memory (RAM) or greater.
- 80 GB hard disk or larger.

- Super VGA (SVGA) or higher resolution monitor capable of a screen resolution of at least 1024 x 768 pixels, at least 256-color display, and a video adapter with at least 4 MB of memory.
- Bootable DVD-ROM drive.
- Mouse or compatible tracking device.
- Network adapter and cabling connecting each classroom computer.
- Network interface card and network cabling.
- IP addresses that do not conflict with other portions of your network.
- Internet connectivity is not required, but is recommended.
- The instructor computer will need a display system to project the instructor's computer screen.

Software Requirements

Each computer requires the following software:

- Microsoft Windows Server 2008 R2, Enterprise Edition, with sufficient licenses.
- Microsoft Baseline Security Analyzer version 2.2 (MBSASetup-x64-EN.msi), available from www.microsoft.com/downloads/en/details.aspx?displaylang=en&FamilyID=02be8aee-a3b6-4d94-b1c9-4b1989e0900c. (You will need to download this tool from a valid copy of Microsoft Windows.)
- The Microsoft Windows Malicious Software Removal Tool (KB890830), available from www.microsoft.com/downloads/en/details.aspx?FamilyID=585d2bde-367f-495e-94e7-6349f4effc74.
- The Microsoft Network Monitor 3.4 (NM34_x64.exe) available from www.microsoft.com/downloads/en/details.aspx?FamilyID=983b941d-06cb-4658-b7f6-3088333d062f&displaylang=en
- Security Update Windows KB2259539 (Windows6.1-KB2259539-x64.msu) available from www.microsoft.com/downloads/en/details.aspx?FamilyID=4eaf707a-e042-483e-a9b6-c2777f18c431 or by searching for KB2259539 on the microsoft.com website.
- Third-party security tools: SuperScan, Cain & Able, and Snort. See the Class Setup section for details.

Course Objectives

Upon successful completion of this course, students will be able to:

- identify the fundamental concepts of computer security.
- identify security threats and vulnerabilities.
- examine network security.
- manage application, data, and host security.
- identify access control and account management security measures.
- manage certificates.
- identify compliance and operational security measures.
- manage risk.
- manage security incidents.
- develop a BCP and DRP.

Course Content

Lesson 1: Security Fundamentals

Topic 1A: The Information Security Cycle
Topic 1B: Information Security Controls

Topic 1C: Authentication Methods
Topic 1D: Cryptography Fundamentals
Topic 1E: Security Policy Fundamentals

Lesson 2: Security Threats and Vulnerabilities

Topic 2A: Social Engineering
Topic 2B: Physical Threats and Vulnerabilities
Topic 2C: Network-Based Threats
Topic 2D: Wireless Threats and Vulnerabilities
Topic 2E: Software-Based Threats

Lesson 3: Network Security

Topic 3A: Network Devices and Technologies
Topic 3B: Network Design Elements and Components
Topic 3C: Implement Networking Protocols
Topic 3D: Apply Network Security Administration Principles
Topic 3E: Secure Wireless Traffic

Lesson 4: Managing Application, Data, and Host Security

Topic 4A: Establish Device/Host Security
Topic 4B: Application Security
Topic 4C: Data Security
Topic 4D: Mobile Security

Lesson 5: Access Control, Authentication, and Account Management

Topic 5A: Access Control and Authentication Services
Topic 5B: Implement Account Management Security Controls

Lesson 6: Managing Certificates

Topic 6A: Install a CA Hierarchy
Topic 6B: Enroll Certificates
Topic 6C: Secure Network Traffic by Using Certificates
Topic 6D: Renew Certificates
Topic 6E: Revoke Certificates
Topic 6F: Back Up and Restore Certificates and Private Keys

Lesson 7: Compliance and Operational Security

Topic 7A: Physical Security
Topic 7B: Legal Compliance
Topic 7C: Security Awareness and Training

Lesson 8: Risk Management

Topic 8A: Risk Analysis
Topic 8B: Implement Vulnerability Assessment Tools and Techniques
Topic 8C: Scan for Vulnerabilities
Topic 8D: Mitigation and Deterrent Techniques

Lesson 9: Managing Security Incidents